



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,195	06/30/2001	Ronald B. Williams	AUS920010245US1	7559

7590 12/15/2004

Joseph R. Burwell
Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, TX 78755-8022

EXAMINER

AHMED, FAROOQUE

ART UNIT	PAPER NUMBER
----------	--------------

2157

DATE MAILED: 12/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center">Office Action Summary</p>	Application No. 09/896,195	Applicant(s) WILLIAMS, RONALD B.	
	Examiner Farooque Ahmed	Art Unit 2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 June 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>06/20/01</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The action is response to application filed on 10/04/01. Claims 1-24 are pending.
Claims 1-24 represent Method and system for secure server-based session management using single-use HTTP cookies

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

2. The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).
3. Reiche teaches the invention substantially as claimed includes Remote user Authentication system and methods with secured HTTP. (See abstract).

As claim 1, Reiche teaches a method for controlling access to protected resources within a distributed data processing system, the method comprising:

receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client (see col 4.

Lines, 55-60; col.10, lines15-67, Reiche disclose client desire a file resources located in customer server where cookies with client);

validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client (see col. 4, lines 50-67,Reiche disclose cookies customer server grant transaction ID to identified session with user);

generating a response to the request and refreshing the single-use token(see col 11, lines1-45 Reiche disclose generate a new cookies by server for the user);

sending the response and the refreshed single-use token to the client (see col. 11, lines1-45, Reiche disclose new cookies from customer server is forward to client browser).

As to claim 2, Reiche teaches the method as recited in claim1, further comprising:

determining that the single-use token is a service token, wherein a service token is issued by the first server (see col.10,lines40 –67; col 11.lines, Reiche disclose cookies determined transition ID in HTTP customer server);

refreshing the single-use service token at the first server (see col.10,lines 40 –67;
col 11,Reiche disclose new cookies transition ID in customer server).

As to claim 3, Reiche teaches the method as recited in claim1, wherein the
session information in the single-use token is a session key (see col. 4, lines 50 -67
Reiche disclose server exchange session data through HTTP with ID stored in URL).

As to claim 4, Reiche teaches the method as recited in claim1,
determining that the single-use token is a domain token(see col 8, lines 25-35
cookies is valid for customer server);

generating a client authorization credential request (see col 8, lines 25-67
detained client request to the file based on ID);

sending to a second server the client authorization credential request, the single-
use domain token associated with the client or the user of the client (see col 5, lines 1-
53, Reiche disclose customer server exchange user ID information authentication
server where HTTP associated with client);

a single-use domain token associated with the first server, wherein the first
server and the second server are operated within a common domain (see col.10, lines
17-67, Reiche disclose cookie in Http customer server and authentication server
network).

As to claim 5, Reiche teaches the method as recited in claim1,
validating at the second server the single-use domain token associated with the
client or the user of the client and the single-use domain token associated

with the first server (see col. 10 lines 5-67, Reiche disclose Authentication server and cookies with client information send to customer server);

generating the client authorization credential (See col 8 lines 25-67 Reiche disclose determined client request to the file based on ID);

refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server (see col 11, lines 11-45, Reiche disclose new cookies to authentication server where user information is send to customer server).

sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, the refreshed single-use domain token associated with the first server (see col 10 lines 5-67, Reiche disclose send client information to authentication server through the cookies from customer server).

As to claim 6, Reiche teaches the method as recited in claim 1, where storing the client authorization credential at the first server; generating a single-use service token associated with the client or the user of the client (see col. 5, lines 1-53 col 10, lines 1-49 Reiche disclose customer server getting client information through HTTP data);

sending to the client the single-use service token along with the response and the single-use domain token (see col. 5, lines 1-53 col 10, lines 1-49 Reiche disclose send information to client through cookies HTTP).

As to claim 7, Reiche teaches the method as recited in claim 1, further comprising:

receiving a login request from the client at the second server;
challenging the client to provide authentication data (see col. 5, lines 1-40, col. 10, lines 1-40);
Reiche discloses authenticating server authenticating challenged to the user to display the User ID):

receiving authentication data from the client; authenticating the client (see col. 5, lines 1-40, Reiche discloses authentication server receive user information):

generating a single-use domain token associated with the client or the user of the client; (see col. 10 lines 15-67, Reiche discloses cookies with user ID);

generating an authentication response (see col. 5, lines 1-40 Reiche discloses authentication server responses to user);

sending the authentication response and the single-use domain token to the client. (see col. 5, lines 1-40 Reiche discloses send cookies with ID to user);

As to claim 8, Reiche teaches the method as recited in claim 1, further comprising:

determining that the login request is a redirected request from the first server;
(see col 5 lines 30-67 Reiche discloses ID is redirected from authentication server to customer server);

modifying the authentication response to redirect the client to the first server (see col 5 lines 30-67 Reiche disclose customer server determined the session based on user ID when its redirected).

Reiche teaches the invention substantially as claimed includes Remote user Authentication apparatus and methods with secured HTTP. (See abstract).

As to claim 9, Reiche teaches an apparatus for controlling access to protected resources within a distributed data processing system the apparatus comprising:

means for receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client (see col 4. Lines 55-60; col.10, lines15-67, Reiche disclose client desire a file resources located in customer server where cookies with client);

means for validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client; see col. 4, lines50-67,Reiche disclose cookies customer server grant transaction ID to identified session with user);

means for generating a response to the request for refreshing the single-use token(see col 11, lines1-45 Reiche disclose generate a new cookies by server for the user);

and means for sending the response and the refreshed single-use token to the client (See col.11 lines 1-45, Reiche disclose new cookies is send from customer server to user).

As to claim 10, Reiche teaches apparatus as recited in claim 9, further comprising:

means for determining that the single-use token is a service token, wherein a service token is issued by the first server; (see col.10,lines40 –67; col 11.lines, Reiche disclose cookies determined transition ID in HTTP customer server).

means for refreshing the single-use service token at the first server(see col.10,lines 40 –67; col 11,Reiche disclose new cookies transition ID in customer server);

As to claim 11, Reiche teaches apparatus as recited in claim 9, further comprising wherein the session information in the single-use token is a session key (See col. 4, lies 50 -67 Reiche disclose server exchange session data through HTTP with ID stored in URL).

As to claim 12, Reiche teaches apparatus as recited in claim 9, further comprising:

means for determining that the single-use token is a domain token (see col 8, lines 25-35, Reiche disclose cookies is valid for customer server);

means for generating a client authorization credential request (see col 8, lines 25-67 Reiche disclose determined client request to the file based on ID);

means for sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client (see col 5, lines 1-53, Reiche disclose customer server exchange user ID information authentication server where HTTP associated with client);

a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain (See col.10, lines 17-67, Reiche disclose cookie in Http customer server and authentication server in network).

As to claim 13, Reiche teaches apparatus as recited in claim, 12 further comprising:

means validating at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server (see col. 10 lines 5-67, Reiche disclose Authentication server and cookies with client information send to customer server);

means generating the client authorization credential (See col 8 lines 25-67 Reiche disclose determined client request to the file based on ID);

means refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server (see col 11, lines 11-45, Reiche disclose new cookies to authentication server where user information is send to customer server).

means sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, the refreshed single-use domain token associated with the first server (see col 10 lines 5-67, Reiche disclose send client information to authentication server through the cookies from customer server).

As to claim 14, Reiche teaches apparatus as recited in claim, 13,further comprising:

means for storing the client authorization credential at the first server;
means for generating a single-use service token associated with the client or the user of the client (see col. 5, lines 1-53 col 10, lines 1-49, Reiche disclose customer server getting client information through HTTP data);

means for sending to the client the single-use service token along with the response and the single-use domain token (See col. 5, lines 1-53 col 10, lines 1-49 Reiche disclose send information to client through cookies HTTP).

As to claim 15, Reiche teaches apparatus as recited in claim 9,further comprising:

means receiving a login request from the client at the second server;
challenging the client to provide authentication data(see col. 5, lines1-40,col.10,lines Reiche disclose authenticating server authenticating challenged to the user to display the User ID):

means receiving authentication data from the client; authenticating the client (see col. 5, lines1-40, Reiche disclose authentication server receive user information):

means generating a single-use domain token associated with the client or the user of the client;(see col. 10 lines15-67, Reiche disclose cookies with user ID);

means generating an authentication response(see col. 5, lines1-40 Reiche disclose authentication server responses to user);

means sending the authentication response and the single-use domain token to the client(see col. 5, lines1-40 Reiche disclose send cookies with ID to user).

As to claim 16, Reiche teaches apparatus as recited in claim15, further comprising further comprising:

means for determining that the login request is a redirected request from the first server; (see col 5 lines 30-67 Reiche disclose ID is redirected from authentication server to customer server);

means for modifying the authentication response to redirect the client to the first server (see col 5 lines 30-67 Reiche disclose customer server determined the session based on user ID when its redirected);

Reiche teaches the invention substantially as claimed includes Remote user Authentication system and methods with secured HTTP. (See abstract).

As claim 17, Reiche teaches a computer program product on a computer readable medium for controlling access to protected resources within a distributed data processing system, the computer program product comprising:

Instructions for receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the

client (see col 4. Lines 55-60; col.10, lines15-67, Reiche disclose client desire a file resources located in customer server where cookies with client);

Instructions for validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client (see col. 4, lines50-67, Reiche disclose cookies customer server grant transaction ID to identified session with user);

Instructions for generating a response to the request and refreshing the single-use token (see col 11, lines1-45 Reiche disclose generate a new cookies by server for the user);

sending the response and the refreshed single-use token to the client (see col.11lines 1-45, Reiche disclose new cookies from customer server is send to user).

As to claim 18, Reiche teaches computer program product as recited in claim17, further comprising further comprising;

determining that the single-use token is a service token, wherein a service token is issued by the first server (see col.10,lines40 –67; col 11.lines, Reiche disclose cookies determined transition ID in HTTP customer server).

refreshing the single-use service token at the first server (see col.10,lines 40 –67; col 11,Reiche disclose new cookies transition ID in customer server);

As to claim 19, Reiche teaches computer program product as recited in claim17, further comprising wherein the session information in the single-use token is a session

key (see col. 4, lines 50-67 Reiche disclose server exchange session data through HTTP with ID stored in URL).

As to claim 20, Reiche teaches computer program product as recited in claim 17, further comprising further comprising;

Instructions for determining that the single-use token is a domain token (see col 5, lines

Instructions for generating a client authorization credential request (see col 8, lines 25-67 determined client request to the file based on ID);

Instructions for sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client (see col 5, lines 1-53, Reiche disclose customer server exchange user ID information authentication server where HTTP associated with client);

Instructions for a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain (See col. 10, lines 17-67, Reiche disclose cookie in Http customer server and authentication server network).

As to claim 21, Reiche teaches computer program product as recited in claim 17, further comprising further comprising;

instructions for validating at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server (see col. 10 lines 5-67, Reiche disclose Authentication server and cookies with client information send to customer server);

instructions for generating the client authorization credential (See col 8 lines 25-67 Reiche disclose determined client request to the file based on ID);

instructions for refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server (see col 11, lines 11-45, Reiche disclose new cookies to authentication server where user information is send to customer server).

instructions for sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, the refreshed single-use domain token associated with the first server (see col 10 lines 5-67, Reiche disclose send client information to authentication server through the cookies from customer server).

As to claim 22, Reiche teaches computer program product as recited in claim 21, further comprising further comprising;

instructions for storing the client authorization credential at the first server; generating a single-use service token associated with the client or the user of the client (see col. 5, lines 1-53 col 10, lines 1-49 Reiche disclose customer server getting client information through HTTP data);

instructions for sending to the client the single-use service token along with the response and the single-use domain token(see col. 5, lines 1-53 col 10, lines 1-49 Reiche disclose send information to client through cookies HTTP).

As to claim 23, Reiche teaches computer program product as recited in claim17,
further comprising further comprising;

instructions for receiving a login request from the client at the second server;
challenging the client to provide authentication data(see col. 5, lines1-40,col.10,lines
Reiche disclose authenticating server authenticating challenged to the user to display
the User ID):

instructions for receiving authentication data from the client; authenticating the
client;(see col. 5, lines1-40, Reiche disclose authentication server receive user
information):

instructions for generating a single-use domain token associated with the client
or the user of the client;(see col. 10 lines15-67, Reiche disclose cookies with user ID);

instructions for generating an authentication response(see col. 5, lines1-40
Reiche disclose authentication server responses to user);

instructions for sending the authentication response and the single-use domain
token to the client.(see col. 5, lines1-40 Reiche disclose send cookies with ID to user);

As to claim 24, Reiche teaches computer program product as recited in claim1,
further comprising:

instructions for instructions for determining that the login request is a redirected
request from the first server; (see col 5 lines 30-67 Reiche disclose ID is redirected from
authentication server to customer server);

instructions for instructions for modifying the authentication response to redirect the client to the first server(see col 5 lines 30-67 Reiche disclose customer server determined the session based on user ID when its redirected).

As to claim 24, Reiche teaches computer program product as recited in claim 23, further comprising further comprising;

instructions for determining that the login request is a redirected request from the first server; (see col 5 lines 30-67 Reiche disclose ID is redirected from authentication server to customer server);

instructions for modifying the authentication response to redirect the client to the first server (see col 5 lines 30-67 Reiche disclose customer server determined the session based on user ID when its redirected).

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farooque Ahmed whose telephone number is 703-605-4212. The examiner can normally be reached on M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (703)308-7562. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

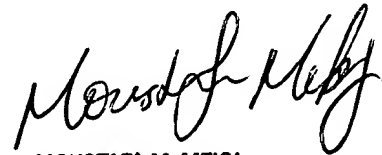
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

Art Unit: 2157

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MOUSTAF A M. MEKY
PRIMARY EXAMINER